# CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

## INTRODUCTION

1. I, Aaron Eastham, am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since 2018. I am currently assigned to the Detroit Field Office, Grand Rapids Resident Agency. During my employment with the FBI, I have conducted investigations involving violations of federal criminal laws, including violations related to child exploitation and pornography. I am familiar with the various statutes of Title 18, United States Code, Chapter 110, which addresses the exploitation and other abuse of children, including violations pertaining to aggravated sexual abuse (18 U.S.C. § 2241(c)), coercion and enticement of minors (18 U.S.C. § 2422(b)), and interstate travel for purposes of engaging in illicit sexual conduct (18 U.S.C. § 2423(b)). I am a federal law enforcement officer and, therefore, authorized by the Attorney General to request a Search Warrant under Federal Rule of Criminal Procedure 41.

2. I make this Continuation in support of an Application for a Search Warrant for the residence of **2753 Duff Road, Twin Lake, Michigan 49457** (hereinafter the 'SUBJECT PREMISES") and the person of **RAYMOND DALE CARR, JR.,** to search for evidence of the online enticement of minors and travel with intent to engage in illicit sexual conduct.

3. The statements contained in this Continuation are based upon information acquired during my investigation, as well as information provided by others such as police officers, task force officers (TFO's) and special agents of the FBI. Because this

Continuation is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that there is evidence of criminal activity in violation of 18 U.S.C. § 2241(c)), 18 U.S.C. § 2422(b), and 18 U.S.C. § 2423(b) at the SUBJECT PREMISES as described in **Attachment A.**

**PROBABLE CAUSE FOR SEARCH WARRANT**

4. On October 8, 2020, the Harris County (TX) Sheriff's Office was dispatched to the residence of the mother of a minor female, identified as MV1 (birth year of 2009). MV1 advised her mother that she had been involved in an online relationship with an adult male known as "Jay Carr", whom she believed resided in Michigan. MV1 stated that she and CARR had been communicating via TikTok as well as text message. MV1 also detailed an occasion on or about September 5, 2020, during which CARR traveled to Texas from Michigan and engaged in sexual intercourse with MV1. MV1 advised her mother that CARR had picked her up at a park near her residence, and he then drove her to the Super 8 Hotel located on Huffmeister Road. MV1 stated CARR performed oral sex on her and that CARR inserted his penis into her vagina.

a. The TikTok application allows users to create a short video of themselves which often feature music in the background. Users can also add their own sound on top of the background music. To create a music video with the app, users can choose background music from a wide variety of music genres and record a video of up to 15 seconds long with speed adjustments

before uploading it to share with others on TikTok or other social platforms. The TikTok application can be accessed both by cellular phone and computer.

5. On or about October 26, 2020, SA Robert J. Guerra of FBI Houston was made aware of the situation involving MV1 and CARR. SA Guerra contacted the mother of MV1 and on October 28, 2020, was able to obtain MV1's cellular devices. During the initial review of MV1's Apple iPhone, there were several text messages between MV1 and an individual saved as "Meh Babyyyy (Jay)", telephone number 231-670-9080, which was identified as belonging to CARR.

6. Further analysis of MV1's iPhone revealed a messaging conversation between MV1 and TikTok user "ROCKINDAD1" that began at 03:25 on September 4, 2020. The online profile for "ROCKINDAD1" included the name "Jay Carr" as well as several pictures clearly identifying the user as RAYMOND CARR. In the conversation on September 4, 2020, CARR asked MV1, "Are you up baby," and then added, "I think I'm stopped for couple three hours I'm in Missouri."

7. In a text message sent later by "Meh Babyyyy (Jay)" to MV1, CARR stated, "Do you know 1 week ago today right now we were laying on my bed making out." There were additional messages indicating that CARR planned to come see MV1 again in November, which was "9 ½ weeks" away. CARR discussed wanting to have sex with MV1 when he came back, and he also made the following statements that appeared to be a reference to his visit in September: "I want back inside you so bad." "Because you taste so good. Because you bite me. Because I love licking the inside of your kitty. Because you

suck me good. Because I like the way you stroke me. Did. Because the way we 69 was best."

8. SA Guerra observed at least two instances where CARR acknowledged that MV1 is in fact under the age of 18. In one text message sent by CARR on September 10, 2020, CARR stated, "I really love you babe that's why I get so upset because I'm 57 years old hopelessly in love with a 13-year-old and nobody understands me." In another text message, CARR told MV1 that he told his son about their relationship. CARR stated, "He knows you are underage", and "Just not what age". In another text message to MV1, CARR explained how he told his daughter that he was in a relationship. CARR stated the following about his conversation with his daughter: "Don't know if she would feel the same way knowing you are 6 mos older than her…..ha ha but I'll take what I can get. Lol". MV1 responded, "Ha ha I'm 11" and then CARR answered, "Yep that's right".

9. SA Guerra observed another text message sent by CARR on September 19, 2020, where CARR stated, "14 days ago, right at this moment, I picked you up and we met irl for the 1st time. From the moment I saw your face, I was deeply IN LOVE with you. I knew it before, but it really confirmed and submitted itself into my heart when I saw you. When you got in my car and we took off and you poked my arm to make sure I was real, that set off electricity through my heart of such joy & love." From my training and experience, I know that irl is short for in real life. SA Guerra also observed two pictures of what appears to be CARR's hand wearing a dark colored ring, followed by another picture of what appears to be MV1's hand, wearing the same type of ring. In the

text message exchange between CARR and MV1, SA Guerra observed several pictures sent by CARR where he showed his face.

10. MV1's mother confirmed the date that MV1 was picked up by CARR near her home as September 5, 2020. MV1's mother also provided SA Guerra with a dark colored ring that MV1 had been wearing. MV1 advised her mother that CARR had given the ring to her when he picked her up. MV1's mother stated that MV1 had initially advised CARR that she was 13 years of age, but then eventually told him she was actually 11.

11. On October 28, 2020, SA Guerra contacted the management at the Super 8 Hotel located at 10710 Huffmeister Road, Houston, Texas 77065, which is located in the Southern District of Texas. The management was able to confirm that a Raymond Dale CARR had booked a two-night stay via www.Expedia.com. CARR checked into the hotel on September 4, 2020, and checked out on September 6, 2020. CARR provided a copy of his Michigan Driver's License. The name on the driver's license was Raymond Dale CARR, Jr, with the date of birth in May 1963 and the address of **2753 Duff Road, Twin Lake, Michigan**. The telephone number provided to the front desk of the Super 8 Hotel was 231-670-9080. The adult male's face pictured in the Michigan Driver's License provided by CARR to the Super 8 Hotel appears to be the same adult male pictured in the images sent during the conversations between CARR and MV1. Additionally, the telephone number provided to the Super 8 Motel on September 4, 2020 is the same telephone number MV1 was communicating with via text message.

a. Expedia.com is an Internet website that allows people to book hotel rooms among other things. Such online bookings are routinely made with desktop and laptop computers, and due to CARR's alleged plans to visit MV1 in November, evidence of past and future travel plans to commit the subject offenses may be found on electronic devices at the SUBJECT PREMISES.

12. A check of a publicly available database shows the most recent address for Raymond Dale CARR, Jr., as **2753 Duff Road, Twin Lake, Michigan**. The same database shows the telephone number being assigned to Raymond Dale CARR, Jr. at the same address on Duff Road.

13. Since the messaging conversations appear to indicate that CARR returned to the SUBJECT PREMISES after his travel to meet with MV1, and their conversations still continued through at least September 22, 2020, there is probable cause to believe that digital evidence related to the subject offenses still exists at the SUBJECT PREMISES.

14. MV1's iPhone also revealed evidence that multiple FaceTime video calls were had between CARR and MV1 between the dates of September 3, 2020 and September 23, 2020. It is not uncommon for a participant of these types of calls to capture screen shot photos or screen recorded videos from those calls, and store them on their electronic devices.

a. FaceTime is an application available on Apple iPhones and Apple computers. It allows two users to engage in video calls. In my training and experience, I have learned that individuals commonly back up their cellular phones using other electronic devices, particularly computers. If a

computer containing that backup is located, a computer forensic analyst is typically able to retrieve the stored information and learn what was on the cellular phone at the time it was backed up.

15. During an interview of CARR's minor daughter by Child Protective Services (CPS), it was discovered that CARR owned a personal computer that is password protected. CARR's daughter had her own user account on the computer, and she did not know the password to CARR's user account. According to information gained from CPS, CARR spends a lot of time on his computer.

**SPECIFICS OF SEIZING AND SEARCHING COMPUTER SYSTEMS**

16. Computers and Internet-capable devices such as tablets and cellular telephones facilitate access to messaging applications which could be used to locate and communicate with minors online for the purposes of enticement. The Internet affords various platforms, through messaging applications, forums, websites, and social media, to connect with individuals, to include minors, across the world, in a relatively secure and anonymous fashion.

17. Storage capacity of computers and portable storage media, such as USB or thumb drives, has grown tremendously within the last several years. These drives can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive. Advances in technology have significantly reduced the size of digital storage devices such that now large numbers of digital files can be stored on media that will fit in a person's pocket, on a keychain, or in any number of easily transportable and concealable places. An individual can now easily carry on his or her person storage

media that contains thousands of files, including images, chat logs, video files, and full-length movie files.

18. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

19. A forensic examiner often can recover evidence that shows whether a computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not allocated to an active file or that is

unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten.

20. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

21. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

22. In order to retrieve data fully from a computer system, the analyst needs all storage devices as well as the central processing unit (CPU). In cases involving photographs, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

23. To examine the computer and digital media properly, it may also be necessary to seize certain other items including documentation of programs, passwords, notes, or even specialized hardware. Therefore, this warrant seeks permission to seize

not only the digital storage media and to search it for evidence in the form of images or videos, stored emails associated with the receipt and distribution of such images, and any chat or other text files relating to contact with children, but also requests permission to seize all hardware, software, and computer security devices necessary to access and examine the computer storage media. Peripheral equipment including printers, routers, modems, network equipment used to connect to the Internet may also contain evidence of what devices were used to connect to the Internet, who used those devices, and what actions the person(s) performed while using such devices.

24. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

25. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the

forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

26. Attempts will be made to preview items on-scene, in order to exclude items unlikely to contain evidence or individuals with no involvement in the subject offenses. Items determined on-scene not to contain items listed in Attachment B will be left at the SUBJECT PREMISES. The remaining items will be seized and searched for further review or forensic examination and will be returned as soon as reasonably possible if they are determined not to contain evidence listed in Attachment B.

27. Retention of any computers would be warranted, if any CP is found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. §§ 2253(a)(3) and 2254(a)(2).

28. I am aware that the recovery of data by a computer forensic analyst takes significant time. For this reason, the Return inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the Return will not include evidence later examined by a forensic analyst.

**REQUEST FOR AUTHORIZATION TO**
**UNLOCK DEVICES WITH FINGERPRINTS OR FACE ID**

29. Based on my knowledge and experience, I know that certain cellular telephones, including Apple iPhones, may be locked and/or unlocked by personal

identification numbers (PIN), gestures or motions, and/or with biometric features, such as thumb and fingerprint recognition (collectively, "fingerprint ID") and/or facial recognition ("facial ID").

30. If a user enables the fingerprint ID unlock feature on a device, he or she can register several fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's sensor, which typically is found on the front of the device. In my training and experience, users of devices that offer fingerprint ID or facial ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

31. In some circumstances, a fingerprint or face cannot be used to unlock a device, and a passcode or password must be used instead. Depending on the configuration of the security settings on the phone, the opportunity to unlock the device via fingerprint ID or facial ID exists only for a short time. Fingerprint ID and facial ID also may not unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) several unsuccessful attempts to unlock the device are made.

32. The passcode or password that would unlock the device(s) found during the search is not known to law enforcement. Thus, it will likely be necessary to press the

finger(s) of the user(s) or present the face of the user(s) of the device(s) found during the search to the device's fingerprint ID or facial ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via fingerprint ID or facial ID is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

33. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a device via the fingerprints on thumbs or index fingers.

34. Based on the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of RAYMOND CARR to the fingerprint ID sensor or to present his face to the facial ID sensor of any his seized device(s) to attempt to unlock the device in order to search the contents as authorized by this warrant.

## CONCLUSION

35. Based on the information provided above, I respectfully submit there is probable cause to believe that RAYMOND CARR used digital devices at the SUBJECT PREMISES to facilitate illegal activities, and that a further search of RAYMOND DALE CARR, JR. and the SUBJECT PREMISES will reveal additional evidence relating to aggravated sexual abuse (18 U.S.C. § 2241(c)), coercion and enticement of minors (18 U.S.C. § 2422(b)), and interstate travel for purposes of engaging in illicit sexual conduct (18 U.S.C. § 2423(b))the "subject offenses."

36. Wherefore, by this Continuation and Application, I respectfully request that the Court issue a Search Warrant authorizing the search of RAYMOND DALE CARR, JR. and the SUBJECT PREMISES described in Attachment A for items listed in Attachment B, and the seizure of those items for the purpose of searching and analyzing them off-site.